REMARKS/ARGUMENTS

In The Claims:

Claims 1–11 are pending in the application.

Claims 1 and 11 have been amended.

Claims 6–10 have been canceled without prejudice.

Claims 12–15 have been added.

Claims 1–5 and 11–15 remain in the application.

Applicant asserts that amended claims 1 and 11, original claims 2–5, and new claims 12–15 are supported by the specification and contain no new subject matter. Furthermore, Applicant reserves the right to pursue in one or more future applications any of the subject matter canceled herein.

Amended Claims 1 and 11 Are Patentable Over the Cited References

Amended claims 1 and 11 are patentable over Stewart[1] in view of Cuomo[2], at least for the reasons and remarks set forth below.

Each of the amended claims 1 and 11 recites, in pertinent part, applying an initialization code to a first chaotic system (having dynamics not determinable solely based on the initialization code) to generate a first key bitstream (the first key bitstream not determinable solely from the initialization code), and applying the same initialization code to a second chaotic system, identical to the first chaotic system, to drive the second chaotic system into synchrony with the first chaotic system, thereby allowing the second chaotic system to reproduce the first key bitstream.

[1] U.S. Patent No. 5,592,555.
[2] *Synchronization of Lorentz-Based Chaotic Circuits with Applications to Communications*, IEEE Transactions on Circuits and Systems, Vol. 40, No. 10, pp. 626–633, October 1993.

Amended claims 1 and 11 also recite that the initialization code causes the first chaotic system to assume a periodic orbit. Support for this amendment to claims 1 and 11 can be found in the specification at, for example, line 25, p. 11 to line 2, p. 12.

Stewart fails to teach or suggest anything relating to the employment of chaotic systems for secure communications. Stewart also fails to teach or suggest the use of an initialization code to synchronize two chaotic systems to remotely reproduce an encryption key, as recited in amended claims 1 and 11. Moreover, Stewart does not teach or suggest an initialization code that can cause a chaotic system to assume a periodic orbit, as recited in the amended claims 1 and 11.

Each of the amended claims 1 and 11 also recites, in pertinent part, that the initialization code is insufficient to determine the key bitstream. In particular, as explained in the specification, the digital key cannot be reconstructed solely from the information communicated from the first to the second chaotic system. Notably, as explained on p. 3, lines 7–9 of the instant specification, even if the initialization code is intercepted, it cannot solely be used to reproduce either the key bitstream or the chaotic system.

In further contrast to the inventions of claims 1 and 11, where an attacker cannot determine any information about any key due to the recited use of the "initialization code", Stewart explains at col. 7, lines 34–39, an attacker can determine his enciphering key by monitoring the air interface. It is, at least in part, this type of prior art deficiency that the recited use of initialization codes in claims 1 and 11 avoids by not transmitting the key (nor anything solely from which the key can be inferred), and instead recites reproducing the key at the second chaotic system, which is synchronized with the first chaotic system.

Cuomo fails to remedy the deficiencies of Stewart. In contrast to the recited invention, Cuomo teaches using a "drive signal," but Cuomo's "drive signal" is not equivalent to the recited initialization code. Unlike the recited initialization code, which, as described on p. 3, lines 7–9 of the instant specification, reveals no information about the chaotic systems, Cuomo's "drive signal" is a chaotic signal that reveals information about the state and dynamics of the chaotic systems.

Cuomo employs what is commonly referred to as additive chaos masking. A known drawback of additive chaos masking is that an attacker can infer the dynamics of the first chaotic system, determine the masking signal, and subtract the masking signal from the transmitted information to reveal a masked message signal. As the recited invention employs an "initialization code," not a "drive signal," no such dynamic information may be inferred from information transmitted between the first and second chaotic systems. Furthermore, Cuomo is silent on causing a chaotic system to assume a periodic orbit.

For any subset of the following reasons, Applicant respectfully requests that the Examiner pass the amended claims 1 and 11 to allowance

a. Neither Stewart nor Cuomo, nor any combination thereof, teaches or suggests the recited use of an initialization code for causing a chaotic system to assume a periodic orbit;

b. Neither Stewart nor Cuomo, nor any combination thereof, teaches or suggests the recited initialization code, solely from which a key bitstream cannot be determined; and

c. Neither Stewart, nor Cuomo, nor any combination thereof, teaches or suggests the recited initialization code, solely from which dynamics of the first chaotic system (and therefore dynamics of the second chaotic system, which is identical to the first chaotic system) cannot be determined.

Dependent Claims 2–5 and 12–15 Are Patentable Over the Cited References

As claims 2–5 variously depend from claims 1 and 11 and recite further limitations thereon, Applicant also respectfully requests that the Examiner reconsider and withdraw the rejection of the dependent claims. New claims 12–15 depend from amended claim 11 and are rewritten forms of canceled claims 7–10. Applicant respectfully requests that the Examiner allow the new claims 12–15, as the new claims recite further limitations on claim 11, which, as shown by the arguments and remarks put forth above, is patentable over the references cited by the Examiner.

CONCLUSION

In view of the above remarks, Applicant submits that claims 1–5 and 11–15 are in condition for allowance, and requests that the Examiner pass this application to allowance.

If the Examiner believes that a telephone conversation with Applicant's attorney would expedite allowance of this application, the Examiner is invited to call the undersigned.

Dated: 26 October 2004

Respectfully submitted by,

John V. B

John V. Bianco
Registration No.: 36,748
ROPES & GRAY LLP
One International Place
Boston, Massachusetts 02110-2624
(617) 951-7000
(617) 951-7050 (Fax)
Attorney/Agent for Applicant

NOTE: It is believed that fees due in connection with this submission have been appropriately provided. However, if an additional fee amount is due, please charge Deposit Account No. 18-1945, under Order No. CAOT-P02-001, from which the undersigned is authorized to withdraw.